REMARKS

The Examiner has objected the Amendment because it is not in conformance with 37 CFR 1.121. This corrected Amendment includes a clean copy of the claims in conformance with 37 C.F.R. 1.121(c)(1) and 1.121(c)(1)(ii). A marked up copy of the claims is attached to this amendment for the Examiner's convenience and in compliance with 37 C.F.R. 1.121(c)(1)(ii).

The Examiner has rejected claims 5, 7-11, and 13-18 under 35 U.S.C. 102(e) as being unpatentable over Trostle (USP 5,919,257). Claims 9, 10, 17, and 18 are cancelled, and claim 11, upon which claims 13-16 depend is amended herein. The Applicant respectfully traverses this rejection in view of this amendment.

With regard to claim 5, upon which claims 7 and 8 depend, the Applicant specifically recites that the private key is removed from the location of the user after the private key is used. The Examiner asserts that Trostle "discloses destroying any non-volatile record of the private key at the location of the user in (col. 6, lines 4-6)." The Applicant respectfully notes that Trostle teaches the destruction of the user's password at the user terminal at (col. 6, lines 4-6), and not the user's private key. As Trostle teaches, after the user's password is

destroyed, the user's private key is used to create a signature that is based on an authenticator credential. The private key is also subsequently used to encrypt a proof that is sent to the server to complete the authentication process (Trostle, column 6, lines 17-22).

Because Trostle does not teach the removal of the private key from the user terminal after it is used, as specifically claimed in claim 5, the Applicant respectfully requests the Examiner's reconsideration of the rejection of claims 5, 7, and 8 under 35 U.S.C. 102(e) as being unpatentable over Trostle.

With regard to claims 11 and 13-16, claim 11 is amended herein to include the use of the private key for signing and verifying a user's approval of a document. As discussed further below, Trostle teaches the comparison of hash values to verify select executable programs, but is silent with regard to encrypting or decrypting this hash value using the user's private key. Furthermore, Trostle specifically notes that an advantage of his invention is that this verification is performed "transparent to the user" (Trostle, column 3, lines 23-30), and thus cannot be said to represent a user "approval" of the verified program.

Because Trostle does not teach a verification of a user's approval of a document based on an encryption of a hash value based on the user's private key, as specifically claimed in claim 11, the Applicant respectfully requests the Examiner's reconsideration of the rejection of claims 11, 13, 14, 15, and 16 under 35 U.S.C. 102(e) as being unpatentable over Trostle.

The Examiner has rejected claims 1, 3, and 4 under 35 U.S.C. 103(a) as being unpatentable over Trostle. Claim 1 is amended herein to correspond to former claim 3, written in independent form, and claims 3 and 4 are cancelled. The Applicant traverses the rejection of claim 1 in view of this amendment.

Claim 1 is amended herein to include the use of the private key that is transmitted from the server for signing and verifying a user's approval of a document. As noted above, Trostle teaches the comparison of hash values to verify select executable programs, but is silent with regard to encrypting or decrypting this hash value using the user's private key, and specifically notes that an advantage of his invention is that this verification is performed "transparent to the user". The Examiner asserts that Trostle teaches this user-approval and verification process at FIG. 6; column 2, lines 44-60; and column 6,

lines 10-25. The Applicant respectfully notes that FIG. 6 does not illustrate an encryption of a hash value, as specifically taught and claimed by the Applicant. The Applicant respectfully notes that column 2, lines 44-60, does not reference a user-approval process, and does not teach an encryption of the hash value, as specifically taught and claimed by the Applicant. The Applicant respectfully notes that column 6, lines 10-25 also does not reference a user-approval process, and does not teach an encryption of the hash value, as specifically taught and claimed by the Applicant. The text at column 6, lines 10-25 presents the login authentication process, wherein the user's private key is used to encode an authenticator credential to form a signature, and to encode a proof that is used to verify the user password. Trostle notes that the signature (not the user's private key) is subsequently used to assist in the validation of packets transmitted by the user's terminal, but provides no further details as to this process.

Because Trostle neither teaches nor suggests a encryption of a hash value to verify a user approval of a document, as specifically claimed by the Applicant, the Applicant respectfully requests the Examiner's

reconsideration of the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Trostle.

The Examiner has rejected claims 2, 6, 12, 19, and 20 under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier ("Applied Cryptography"). The Applicant respectfully traverses this rejection based on the remarks above regarding claims 1, 5, and 11, upon which each of the rejected claims depend.

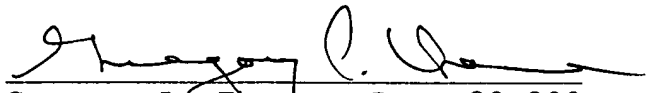
As noted above, claims 1 and 11 have been amended to include the use of a user's private key that is transmitted from a server to encrypt a hash value corresponding to a document that is approved by a user, and to use the encrypted hash value to verify the user's approval. Claim 5 has been amended to include the removal of the user's private key from the location of the user after the user's private key is used.

In view of this amendment, the Applicant respectfully requests the Examiner's reconsideration of the rejection of claims 2, 5, 12, 19, and 20 under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier.

Based on the remarks above, the Applicant respectfully requests the Examiner's reconsideration of each of the rejected claims, and the subsequent allowance of all

pending claims 1-2, 5-8, 11-16, and 19-20 in this application.

Respectfully submitted,



Gregory L. Thorne, Reg. 39,398
Reg. No. 41,508
(914) 333-9665

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER FOR PATENTS
Washington, D.C. 20231

On February 20, 2001

By Naomi Chapa

MARKED-UP CLAIMS

1. (Amended) A method of administration of private keys for a plurality of users for use to encrypt or decrypt items transmitted via a network, there being for each user a respective set of an ID, user identifying information, private key, and public key corresponding to the private key, said method comprising:

receiving via the network a user's ID;

reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user; [and]

sending via the network the encrypted private key, whereby the encrypted private key can be received and decrypted at the location of the user using the user's identifying information[.];

receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key; and

verifying the received digital signature by decrypting the digital signature using the user's public key and

comparing the result of this decrypting with an independently computed hash of the document.

11. (Twice Amended) A system for administering private keys and corresponding public keys for a plurality of users, comprising:

computer readable storage means and

a server,

characterized in that:

the storage means includes therein respective IDs and encrypted private keys for the respective users which private keys have been encrypted using respective keys determined from respective user identifying information, and

the server is configured:

to read an encrypted private key from the storage means associated with an ID corresponding to a particular user [and],

to transmit the encrypted private key to the particular user [.],

to receive a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key, and

to verify the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

13. (Amended) A system as claimed in Claim 11, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

14. (Amended) A system as claimed in Claim 12, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

15. (Twice Amended) A system as claimed in Claim 11, characterized in that

the server is further configured[:]

[to read from the storage means a corresponding public key associated with the ID and] to decrypt data received from the particular user using the public key.

16. (Twice Amended) A system as claimed in Claim 12, characterized in that

the server is further configured[:]

[to read from the storage means a corresponding public key associated with the ID and] to decrypt data received from the particular user using the public key.